Remarks

In an Office action mailed October 13, 2006, claims 1-7 were rejected under 35 U.S.C. § 101 on grounds that the claimed invention is directed to non-statutory subject matter.

The Examiner incorrectly stated that the claims recite a method for performing a mathematical function. Instead, the claims actually recite "a method of operating an multiplication circuit…." Thus, the claims are not directed to performing a mathematical function *per se*, but rather to a specific, practical and concrete application in which hardware circuitry ("multiplication circuit", "accumulator", "registers", and "memory") is directed in a sequence of steps involving memory accesses ("loading" and "storing") and operations by a hardware multiplication circuit with accumulator ("multiplying" and "adding") that together allow the circuitry as a whole to "compute the product of two operands". The scope of the claims is, therefore, understood in this real world context of operating the multiplication circuit, with access to memory, according to the particular sequence of steps set forth in the claims. It does not foreclose all use of the underlying mathematical principle or algorithm in the abstract, whether by hand or by machine generally, but only as it relates to the specified concrete operation of a multiplication circuit as claimed.

The Examiner also asserts that "since there is no physical transform to establish a practical application, a useful, concrete and tangible result appears to be lacking." This is incorrect in both respects. There are numerous physical transformations occurring in the method, as claimed. The loading of word-wide operand segments from memory into the at least two registers (RX and RY) of the multiplication circuit involves a physical change of the electronic states of those registers every time a segment is loaded. The act of

multiplying necessarily involves physical transformations of the electronic states within the hardware of the multiplication circuit, otherwise, no outputs ("two-word-wide intermediate products") would be obtained. The adding of intermediate products of the same weight in an accumulator likewise necessarily involves physical transformations of the electronic states with the hardware of the accumulator and wells as physical changes of the electronic states of the to-word input register (RZ) and two-word output register (RR) associated with that accumulator. The storing of accumulated results from the output register (RR) back into the memory involves a physical change of the electronic states of the memory. The particular results physically stored within that memory are functionally related to the operations of the multiplication circuit.

The claimed method implemented in the multiplication circuit hardware provides a useful, concrete and tangible result possessing real world value. The multiplication circuit performs its claimed computation with far fewer memory accesses over that of other multiplication circuits (including the three cited in the Office action). It provides a tangible result that can be stored physically in memory, which can then be accessed for further use. One exemplary use for the claimed method mentioned in the specification is in cryptography. Cryptographic applications generally require that computations be performed upon very wide operands for adequate security (typically at least 256 bits for symmetric cryptosystems or at least 1024 bits for public-key cryptosystems), much wider than the physical computation hardware, where the message blocks, cryptographic keys, and other cryptographic data are treated by the hardware performing the cryptographic application as if they were numeric values. Cryptographic applications tend to be so computationally intensive, involving, for example, polynomial

arithmetic upon very large integer values, that any improvement in efficiency and speed of the computations have very real utility. The present invention offers such an improvement, since each memory access, whether to load an operand segment or store accumulated results, requires one cycle of time over and above the time required for the multiplying and accumulating by the multiplication circuit and accumulator hardware. Fewer memory accesses (a physical operation), means a more efficient and faster computation overall by the hardware.

The rejection under 35 U.S.C. § 101 is believed to be traversed.

Obviousness Rejections

Claims 1-8 were rejected under 35 U.S. C. § 103(a) as being unpatentable over Chevillat et al. (IBM Tech. Disc. B-11.). The Chevillat document was cited for disclosing a 12x12 multiplier unit that can carry out a 12x16 multiplication operation ("extended precision"). This means that at least one operand, namely the 16-bit multiplicand, is wider than the multiplication circuit. The operation is split into two steps. In the first step, the 12 most significant bits of the 16-bit multiplicand are received (by the 12x12 multiplier unit) through the B register. In the second step, the four remaining least significant bits of the multiplicand are received through the B register, right aligned with 8 leading zeros. In both the first and second steps, the 12-bit multiplier is received through the A register. The partial result of the first step is stored in the accumulator. The result of the second partial multiplication is appropriately scaled by a shifter at the multiplier output, then added to the first partial result to obtain a final result in the accumulator.

The Office action asserts that the multiplication circuit of Chevillat et al. comprises: multiplier and multiplicand registers (these are the A and B registers), a multiplier unit, ALU and accumulator. These features are clearly seen in the drawing figure on the front of the cited document. Further, the Office action notes that Chevillat et al. do not show that the accumulator has a size of "three words plus a number of carry bits", as recited in independent claims 1 and 8 of the application, but argues that it would have been obvious to use a accumulator having sufficient size to accommodate that desired final result of the multiplication circuit. Notwithstanding all of those statements, Applicants assert that the claimed invention would not have been obvious because Chevillat et al. fail to disclose or suggest the claimed "specified order" or "sequence" defined in the last indented section of method claim 1, nor a "operations sequencer" controlling that "sequence" as defined in the last two sections of claim 8.

Applicants' multiplication circuit-implemented method and corresponding multiplication circuit with specified operations sequencer is provided to enable computation of very large products of two operands (claim 1: "substantially wider than the multiplication circuit" and "each of the operands composed of a plurality of contiguous word-wide operand segments"), much larger than a mere 16x12 bit (1 ½ words by 1 word) multiplication and much larger than any accumulator could wholly accommodate. Even an operation as small as multiplying 8 words by 8 words operands, provided as an example in Figs. 4 through 5c of the present application, would require at least a wide 16-word accumulator (plus additional carry bits) if it were to be implemented as suggested in Chevillat et al. Many of the operations enabled by the present invention are ever larger (page 11, line 34 - page 12, line 3). Instead of widening the accumulator to

accommodate an entire product result, the accumulator is given a size only wide enough (claims 1 and 8: "output of three words plus a number of carry bits") to accumulate intermediate products in "groups of two adjacent product weights" that are obtained in the defined sequence controlled by the operations sequencer. Because only intermediate products are added in the accumulator, not an entire product, accumulated results are stored back into memory "after accumulating all intermediate products of the specified weight", as set forth in our claims. None of this is described or suggested by the cited document.

Claims 1-8 were also rejected under 35 U.S.C. § 103(a) as being unpatentable over New et al. (U.S. Pat. No. 4,809,212). New et al. was cited for disclosing a 32x32 multiplication circuit having 64-bit operands wider than the multiplication circuit ("double precision"). As noted in the Office action the multiplication circuit comprises multiplier and multiplicand registers (102, 106, 132, 136), a multiplier array (120), and an accumulator (adder 152, shifter 160 and register 166). It is also noted that New et al. do not show the accumulator having a size of three words plus a number of carry bits, as set forth in Applicants' claims - the accumulator of New et al. being 67-bit wide, i.e., two words plus three bits.

New et al. fail to disclose or suggest "loading word-wide operand segments of the two operands in a specified order from the memory into the multiplication circuit, …; wherein the specified order for loading operand segments into said registers is a sequence defined by the intermediate product weights", as specified in Applicants' claim 1, nor the corresponding "operations sequencer" and its defined sequence specified in Applicants' claim 8. Indeed, New et al. has data registers for holding all of the 32-bit portions of the 64-bit double-precision operands, i.e., registers XA and XB for the

multiplicand and registers YA and YB for the multiplier. Thus, it does not really matter to New et al.'s multiplication circuit in what order the operand portions are loaded into the registers.

In contrast, the "substantially wider" (claim 1) operands in the present invention could not be readily stored in registers all at the same time. For example, the relatively modest size 8-word by 8-word example given in Figs. 4 through 5c of the present application would require a total of 16 distinct data input registers (8 for each operand) if applied to the circuit construction described by New et al. The even larger multiplications that are possible with the present invention (page 11, line 34 to page 12, line 3) could not be so accommodated; they would require far too many registers. Instead, of having a separate data register for every operand segment, the present invention makes do with fewer data registers (e.g., RX, RY, RZ, RR in Fig. 3) for "temporarily holding" (claim 1) the operand segments, loading the operand segments "in a specified order" (claim 1) from the memory. (See page 8, lines 1-3, page 8, line 14 - page 9, line 5, and the description of the specified order or operation sequence beginning on page 10.)

The present invention as claimed not only adds intermediate products of the same weight in an accumulator, but also stores accumulated results "back into said memory at least after accumulating all intermediate products of the specified weight". The New et al. patent teaches away from this feature (see, e.g., col. 1, lines 25-37 and 60-68) by noting the slowness of off-chip data transfers. New et al. are able to avoid the need for external storage of temporary results or for any off-chip intermediate data transfers since they are performing a mere double-precision operation. Because at least one of the operands is substantially wider than the multiplication circuit in the present invention,

storage of temporary results (the accumulated intermediate products of the specified weight) back into memory cannot be avoided, but is minimized by the claimed feature of doing the multiplying step "in successive groups of two adjacent product weights". This is not taught nor suggested by the cited New et al. patent.

Claims 1-8 were also rejected under 35 U.S.C. § 103(a) as being unpatentable over Rim (U.S. Pat. No. 5,920,497). Again, like New et al. this is a method and apparatus for performing "double precision" multiplication operations. As the operands are only two words wide, they can be completely stored in just four registers (L1, L0, R1, and R0). Again, the entire product can be accumulated without having to store intermediate results in external memory. The same features of the present invention that were noted in relative to Chevillat et al. and New et al. are also neither taught nor suggested by Rim.

Conclusion

In light of the technical features already claimed, the invention is deemed to be non-obvious and patentable over the cited prior art. Applicants request reconsideration of the claims in view of the arguments made herein. A Notice of Allowance is earnestly solicited.

CERTIFICATE OF MAILING

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted via the Office electronic filing system in accordance with § 1.6(a)(4) on the date shown below.

Signed: Sally Azevedo
Typed Name: Sally Azevedo

Date: February 26, 2007

Respectfully submitted,

David M. Schneck
Reg. No. 43,094

Schneck & Schneck
P.O. Box 2-E
San Jose, CA 95109-0005
(408) 297-9733